



Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0)

This is a human-readable summary of (and not a substitute for) the license. [Adaptación.](#)

Usted es libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato.

Adaptar — remezclar, transformar y construir a partir del material.

La licencianta no puede revocar estas libertades en tanto usted siga los términos de la licencia.

Bajo los siguientes términos:



Atribución — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licencianta.



NoComercial — Usted no puede hacer uso del material con propósitos comerciales.

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Las debilidades en materia de protección de datos personales en la regulación emitida por el Estado colombiano¹

Weaknesses in the protection of personal data in the regulations issued by the Colombian State

José Alejandro Higuera Arias²
Universidad Católica de Colombia

Resumen

La protección de datos personales es un tema que se ha venido fortaleciendo en la mayoría de los Estados, que han considerado relevante adoptar políticas públicas dirigidas a construir parámetros para el tratamiento de datos personales de los individuos. Lo anterior, teniendo en cuenta que tanto en el sector público como en el privado se obtienen datos de las personas por diversos motivos, y en consecuencia es necesario identificar bajo que reglas deben resguardarse estos, fijando de este modo políticas de tratamiento de datos y reserva. Precisamente, la protección de datos personales ha sido un tema objeto de discusión y amplio desarrollo en los Estados, incluso en la actualidad existen normas de tipo comunitario e internacional, lo que hace necesario observar con detenimiento la regulación que al respecto se ha emitido en Colombia, y cuales pueden considerarse como aspectos débiles de la misma, que pueden ser objeto de fortalecimiento por parte de las entidades estatales que regulan la materia.

Palabras Clave: Colombia, Derecho a la privacidad, Datos Personales, Datos Sensibles, Protección de Datos, Regulación.

Abstract

The protection of personal data is an issue that has been strengthening in most of the States, which have considered it relevant to adopt public policies aimed at building parameters for

¹ Artículo de reflexión presentado como requisito para optar al título de Abogado de la Universidad Católica de Colombia, bajo la asesoría del Doctor Marco Emilio Sánchez Acevedo, docente de la facultad de Derecho, 2019.

² Estudiante de Derecho con materias culminadas y en proceso de grado de la Universidad Católica de Colombia, identificado con código estudiantil N° 2110644. Correo electrónico: jahiguera44@ucatolica.edu.do

the processing of personal data of individuals. This, considering that both in the public and private sectors data are obtained from individuals for various reasons, and consequently it is necessary to identify under what rules they should be protected, thus setting data processing and confidentiality policies. Precisely, the protection of personal data has been a subject of discussion and extensive development in the States, even at present there are community and international standards, which makes it necessary to carefully observe the regulations that have been issued in Colombia, and which can be considered as weak aspects of the same, which may be subject to strengthening by the state entities that regulate the matter.

Key words: Colombia, Right to privacy, Personal Data, Sensitive Data, Data Protection, Regulation.

Sumario

Introducción. 1. La protección de datos personales en el derecho internacional e interno. 2. El desarrollo del derecho fundamental al Habeas Data en Colombia. 3. Retos para Colombia frente a la protección de datos personales. Conclusiones. Referencias.

Introducción

Es importante destacar que en el marco del derecho a la intimidad se protege la vida privada de cada individuo, esto dentro del conjunto de libertades que tiene el ser humano. Así entonces, será decisión de cada persona aquellos aspectos que revela de su vida y aquellos que prefiere mantener bajo reserva por uno u otro motivo.

En ese sentido, cabe aclarar que la protección de datos personales se reconoce como una práctica que garantiza los derechos de los individuos, y obliga a las entidades públicas y privadas manejen de manera adecuada los datos personales que por algún motivo llegan a sus bases de datos, y se determinara también por cuanto tiempo podrán tener dicha información en custodia y como se procede a la eliminación de esta (Becerra, et al., 2015).

De igual manera, la protección de datos personales es un derecho reconocido desde el ámbito convencional, en la medida que está contenido en una serie de instrumentos de derecho

internacional que han sido suscritos y ratificados por Colombia, como lo es el Pacto Internacional de Derechos Civiles y Políticos ratificado por Colombia el 29 de octubre de 1969 y la Convención Americana sobre Derechos Humanos que también se ratificó en el ordenamiento jurídico colombiano.

Como se ha evidenciado el compromiso del Estado colombiano con la protección de datos personales es una obligación adquirida desde el orden constitucional y convencional, lo que hace necesario que se generen medidas efectivas para que existan herramientas que garanticen el derecho a la protección de datos personales (Remolina, 2010).

Por su parte, en Colombia, la protección de datos personales se considera un derecho fundamental de acuerdo con lo expresado en el artículo 151 de la Constitución Política de 1991 sobre el derecho a la intimidad y la garantía que debe dar el Estado frente a la recolección, tratamiento y circulación de datos. Al respecto, como lo advierte Torres (2016) la evolución histórica de la protección que se le ha dado a la recolección y tratamiento de datos personales en Colombia, da cuenta de los esfuerzos del Estado, ya que como se observará a continuación el camino recorrido hasta hoy ha sido largo.

Lo expuesto anteriormente, ha permitido centrar el presente artículo de reflexión en la pregunta de investigación siguiente ¿Cuáles son las debilidades en la regulación sobre protección de datos personales en Colombia? El desarrollo de dicho artículo se centrará en el objetivo principal de Identificar los aspectos a fortalecer en materia de regulación sobre protección de datos en Colombia.

Metodología

La metodología mediante la cual se desarrolla el presente artículo de reflexión es esencialmente documental descriptivo para lo cual se utilizó un método de tipo doctrinal y jurisprudencial hermenéutico, (Agudelo, 2018) que revisa diversas fuentes doctrinales y jurisprudenciales para desarrollar los temas propuestos y dar respuesta a la pregunta de investigación.

1. La protección de datos personales en el derecho internacional e interno.

Para comenzar, es importante indicar que la privacidad e intimidad del ser humano, se ha considerado como una esfera esencial en la vida de estos, es por ello por lo que en la Declaración Universal de Derechos Humanos del 10 de diciembre de 1948 se consagran los derechos y libertades de cada individuo, y la protección que debe darse a estos.

Ahora bien, dentro de los derechos contemplados en esta declaración, se encuentra precisamente el derecho a la intimidad que busca proteger la vida privada de cada individuo, esto dentro del conjunto de libertades que tiene el ser humano (Romero, 2008). Por tal razón y en ejercicio precisamente de este derecho, será decisión de cada persona aquellos aspectos que revela de su vida y aquellos que prefiere mantener bajo reserva por uno u otro motivo (Hernández, 2008).

Resulta claro de lo anterior, que los Estados deben proteger el ámbito privado de cada individuo garantizando su derecho a la intimidad personal, por lo que es su deber disponer de los elementos necesarios para esto, emitiendo la regulación pertinente y reglamentando en concreto la información pública y aquella sujeta a reserva.

Sobre el derecho a la intimidad personal, se ha expresado lo siguiente:

El ser humano va estableciendo a lo largo de la vida relaciones de distinta intensidad con sus semejantes y elige con quién quiere compartir aquello que le es más propio, aquello que le hace diferente de cualquier otro individuo, sus secretos. La intimidad, por tanto, representa lo más nuclear del ser humano, y debe ser protegida (Iraburu, 2006, p.91).

Sin duda, en el ámbito actual y teniendo en cuenta el auge que existe sobre tecnologías de la información es importante que exista una completa regulación de la protección a la información personal de cada individuo, teniendo en cuenta las consecuencias que pueden derivarse por la divulgación de datos que personales o sensibles, y la responsabilidad que tendrían las instituciones estatales por los perjuicios que se causen por esta razón.

En esa medida se ha regulado el tema desde el ámbito internacional, comunitario e interno, lo que se desarrollará a continuación.

1.1 Regulación Unión Europea sobre protección de datos personales:

El tema de protección de datos personales se ha regulado desde diversos ámbitos, uno de ellos el marco comunitario como es el caso de la Unión Europea que sobre el tema ha emitido varias directivas privilegiando el derecho que tiene cada persona a que sus datos personales tengan una adecuada custodia.

Así entonces, en primer lugar, existe un Reglamento general de protección de datos (RGPD) que rige a partir del año 2018 y aplica a todos los miembros de la Unión Europea y señala de manera concreta regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas (Puldain, 2017).

En consecuencia. los cambios introducidos mediante este reglamento buscan dar más seguridad a cada una de las personas teniendo en cuenta las innovaciones en materia de tecnologías de la información, que suponen nuevos retos al momento de proteger la información privada y sensible. Ya que como lo explica Castro (2016) la revolución en las comunicaciones y la forma de actuar de los ciudadanos genera un riesgo más alto para los datos personales, por lo que es necesario fijar reglas sobre la forma en que se deben tratar dichos datos personales por parte de quien los recolecta.

Y es que precisamente dicha norma fija de manera taxativa una serie de derechos que tienen los usuarios frente a las empresas o personales que están tratando sus datos personales, entre estos está el derecho a conocer quien tiene su información personal y de qué manera la está tratando.

En segundo lugar, como lo indican Galvis y Salazar (2019) se privilegia el derecho a rectificar los datos y solicitar al responsable del tratamiento de sus datos que suspenda el tratamiento, lo conserve parcial o completamente o realice la portabilidad de estos, suprimir los datos que tiene u oponerse por motivos personales a su tratamiento.



Figura 1. Reglamento General de Protección de Datos Unión Europea. Fuente: SISLEI (2018).

De igual manera, como se logra observar, este reglamento incluye una serie de procedimientos y obligaciones para los responsables del tratamiento de datos personales en el marco de la Unión Europea e impone sanciones de carácter económico, y pago de perjuicios en los casos que se llegaren a causar.

En ese sentido, como lo afirma Fernández (2016) el reglamento de protección de datos diseñado para la Unión Europea busca que exista una protección real y efectiva de la

intimidad de los individuos, y adicionalmente fija una serie de prohibiciones específicas para la recolección y tratamiento de datos que por su sensibilidad no pueden ser tratados, lo que fija un ámbito claro para el ejercicio de las entidades públicas y privadas en tratamiento de datos personales, limitando ciertas materias sensibles y previniendo de esta manera que exista una afectación a los derechos de los individuos.

Ahora bien, visto el análisis anterior, es necesario entrar a analizar que se ha dicho de la protección de datos personales en el Sistema Interamericano de Derechos Humanos, teniendo en cuenta que es el sistema de protección de Derechos Humanos que rige para Colombia, y en cierta medida orienta la regulación interna de los Estados parte.

1.2 Protección de datos personales en el Sistema Interamericano de Derechos Humanos:

En el marco del Sistema Interamericano de Derechos Humanos se ha definido el alcance del derecho a la intimidad y la protección de datos personales, teniendo en cuenta que esto representa la garantía de la privacidad de cada individuo. En ese sentido, la Organización de Estados Americanos (2019) ha expresado lo siguiente:

El concepto de privacidad se encuentra vinculado al de la intimidad que es un derecho garantizado en los principales instrumentos interamericanos y universales de derechos humanos que adquiere en el valle de silicón una dimensión nueva, con retos que exigen un balance entre el derecho a la intimidad del individuo y los avances en el mundo de las TICs. Así lo han reconocido los países de las américas, cuya tendencia muestra la incorporación del derecho a la protección de datos personales en sus ordenamientos constitucionales y el desarrollo de normativa especial en esta materia (p.1).

Precisamente, en el marco de lo anterior este organismo expidió una normatividad modelo sobre la protección de datos personales para que pueda ser consultada y replicada por los Estados en los casos que así lo consideren, para lograr generar un marco de protección del derecho a la intimidad a través de la adecuada custodia y tratamiento de los datos personales.

De igual manera se han señalado los Principios sobre la Privacidad y la Protección de Datos Personales, adoptados en el año 2015 que concretamente hace referencia a la finalidad

legítima de la recolección de datos, la transparencia en el tratamiento, la necesidad del consentimiento para almacenar y tratar dichos datos, la confidencialidad, la seguridad, entre otros.

En este mismo ámbito, como lo señalan Maqueo, Moreno & Recio (2017) la Corte Interamericana de Derechos Humanos ha señalado, Asimismo, el derecho a la privacidad de cada individuo tiene una característica fundamental y es que debe estar exento de cualquier invasión por parte de personas naturales o jurídicas, e incluso autoridades públicas. En esa medida cada Estado debe señalar políticas que señalen concretamente cuáles serán los procedimientos para la obtención, custodia, eliminación y transferencia de datos personales, de modo que no se vulnere el derecho a la intimidad del individuo.

Dicho lo anterior, se procederá a realizar el análisis de la regulación sobre protección de datos personales en Colombia.

2. El desarrollo del derecho fundamental al Habeas Data en Colombia.

La Corte Constitucional ha expresado la importancia del derecho fundamental al Habeas Data desde el pronunciamiento en la sentencia T-414 de 1992 que expresa lo siguiente:

Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares (Corte Constitucional, Sentencia T-414 de 1991[M.P. Ciro Angarita Barón]).

Tal es la importancia del derecho al habeas data que ha sido reconocido en instrumentos de derecho internacional, como el Pacto Internacional de Derechos Civiles y Políticos ratificado por Colombia el 29 de octubre de 1969 y la Convención Americana sobre Derechos Humanos ratificada por Colombia el 31 de julio de 1973, lo que indica que el Estado colombiano debe garantizar el derecho al habeas data para todos los individuos y diseñar mecanismos de protección que le permitan a los ciudadanos ejercer la defensa del mismo (Bazán, 2005).

El tema de protección de datos personales en Colombia se contempló tratando en el Artículo 15 de la Constitución de 1991 donde se hace referencia al derecho a la intimidad que se expuso de manera taxativa en el artículo 15 de la Carta política, que se considera una forma de asegurar la convivencia pacífica entre los ciudadanos y el desarrollo de la personalidad de cada individuo.

En esa medida y el Legislador colombiano, entendiendo que el Estado debe garantizar los derechos fundamentales, entre ellos la intimidad y la protección de datos personales, expidió la “Ley 1266 de 2.008 es una ley de carácter estatutaria, mediante la cual se desarrolla el derecho fundamental de habeas data y establece el procedimiento para su protección” (Gil, 2017, p.20).

Sin embargo, resulto insuficiente teniendo en cuenta que enfoco dicha protección únicamente hacia los sectores comerciales y financieros, circunstancia por la cual fue necesario proferir una nueva normatividad que regulara de manera integral la protección de datos personales (Rojas, 2014).

Es notorio la importancia que se dio sobre el derecho a la intimidad y la protección de datos personales, teniendo en cuenta que estos constituyen un elemento fundamental del derecho a la intimidad personal. Posteriormente se expide la Ley 1581 de 2012 que busca formular las políticas sobre la recopilación de datos y el tratamiento de estos.

En ese aspecto Bautista (2015) señala que la norma antes mencionada reconoce el derecho a la intimidad y la relación que tiene este con la protección de datos personales, razón por la cual se debe privilegiar el derecho de todas las personas de conocer, actualizar y rectificar la información o los datos que se hayan recogido sobre estas en bases de datos para determinados tramites.

Ha indicado la Corte Constitucional, sobre el contenido del derecho de Habeas Data lo siguiente:

De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas –contenidos mínimos- que se desprenden de este derecho encontramos, por lo menos, las siguientes: (i) el derecho de las personas a conocer –acceso- la

información que sobre ellas está recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a un incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos o archivo, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. Como se aprecia la protección del derecho fundamental del habeas data tiene como finalidad la protección de los datos en un mundo globalizado (Corte Constitucional, Sentencia T-260 de 2012, [M.P. Humberto Antonio Sierra Porto]).

Precisamente la Ley 1581 de 2012 se encargó de regular aspectos como los derechos que tienen los titulares respecto de su información, esto teniendo en cuenta que al ser los dueños de esta están en la capacidad de solicitar al responsable de la custodia de los datos que se proceda a su eliminación o se conserve de cierta manera.

Respecto de los derechos que tienen los titulares de la información, la figura 2 que se muestra a continuación elaborada por la Superintendencia de Industria y Comercio muestra de manera clara los mismos.



Figura 2. Derechos del titular de la información. Fuente: Superintendencia de Industria y Comercio (2014)

Es claro entonces que el titular de la información tiene derecho a conocer los datos que ha adquirido una entidad y podrá solicitar que se actualice, se corrija o se suprima si lo considera. De igual manera se hace obligatorio que quien custodie esta información cuente con un permiso del titular de esta, e informe al individuo sobre el uso y tratamiento que le dará a la misma.

El consentimiento para el tratamiento de datos personales puede darse por escrito, de manera verbal, o mediante conductas inequívocas del titular de la información, las cuales permiten concluir a los responsables que se otorgó la autorización, no obstante, el responsable del tratamiento de datos debe estar en capacidad de demostrar la autorización del titular de los datos personales en el caso que se presente una queja en contra de este (Galvis, 2012).

Sin embargo, para el adecuado tratamiento de datos personales debe identificarse la clasificación dada por el legislador en la norma de los tipos de datos que existen y cuáles

serán privados o públicos. Ya que no todos gozan del mismo ámbito de protección precisamente por la categoría en la que los clasifico el legislador.

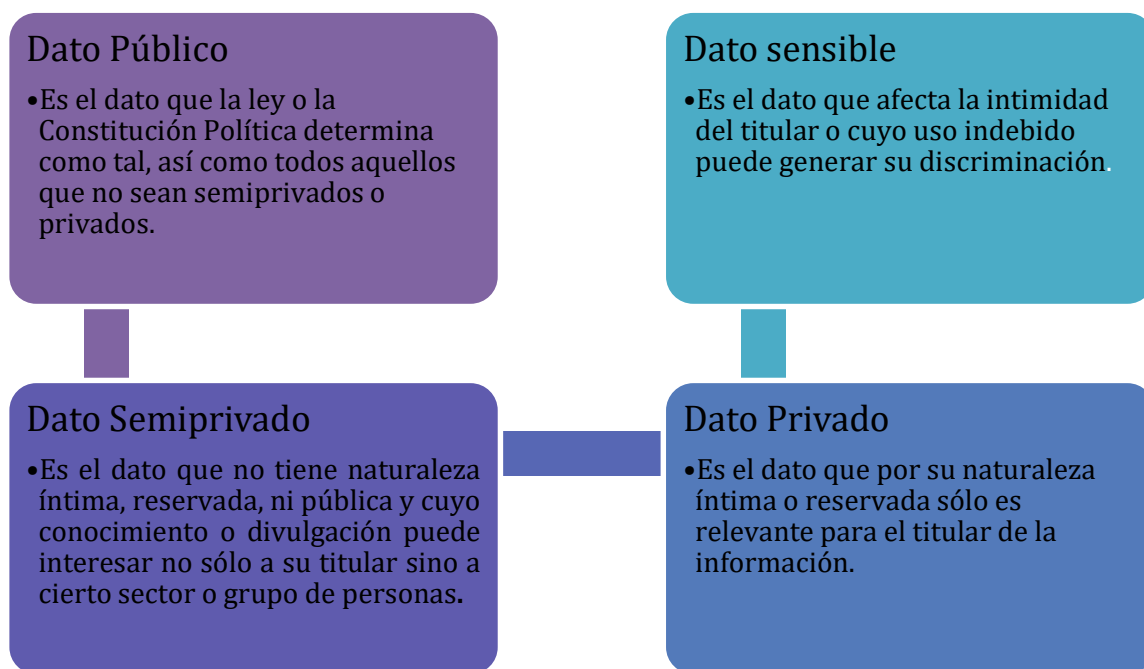


Figura 3. Clasificación de datos. Elaboración propia a partir de información de la Superintendencia de Industria y Comercio (2016).

Lo anterior, es relevante en la medida que los datos públicos no son objeto de la política de tratamiento, custodia y eliminación de datos personales, ni serán objeto de reserva por parte de quien la tiene a su cargo.

Por otra parte, la divulgación que se encuentra restringida es la de aquellos datos privados y sensibles teniendo en cuenta que estos están directamente relacionados con el derecho a la intimidad de cada individuo y es deber del Estado garantizar en todo este derecho constitucional y convencionalmente protegido.

Ahora bien, como reglamentación de la Ley 1581 de 2012 se expide el Decreto 1377 del 27 de junio de 2013 que tuvo como finalidad facilitar la implementación de lo dispuesto en la

Ley estatutaria. Aquí se contemplaron obligaciones expresas para el responsable del tratamiento de datos ya recolectados, y los que se recolectarían con posterioridad a la expedición de esta norma, se hacen precisiones sobre el contenido de las autorizaciones de tratamiento de datos personales y la política de tratamiento de datos personales que debe elaborar cada entidad pública (Buitrago, 2016).

No obstante del marco jurídico mencionado anteriormente, a la fecha, se ha evidenciado que la implementación de esta norma, no ha sido tan eficaz, ni ha cumplido todos los objetivos que se propuso el legislador, la figura 4 evidencia la radiografía de la implementación de la Ley de información dada por la Superintendencia de Industria y Comercio y compilada por el Diario La República, en este se puede observar que las multas establecidas hasta el momento son muy pocas, teniendo en cuenta la violación continua que se hace del derecho al habeas data y la práctica común que se tiene en la actualidad de compartir o vender bases de datos para el ofrecimiento de productos o servicios.



Figura 4. La protección de Datos en Colombia. Fuente: Diario La República (2015).

No obstante, en este ámbito es preciso realizar una crítica, ya que si bien en la mayoría de casos, se presenta la autorización del titular para el tratamiento de la información de acuerdo a lo dispuesto en la política de tratamiento de datos del establecimiento público o privado, la divulgación de la información con otros establecimientos sigue siendo un problema que no ha disminuido con la implementación de la ley, de igual manera el registro de las bases de datos es un mandato que aún no ha tenido la suficiente acogida, por lo cual se ha debido ampliar el plazo en varias ocasiones.

Entendiendo las falencias de lo anterior, se expide el Decreto Único 1074 de 2015, que reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.

Sin embargo, nuevamente en el año 2018, mediante el Decreto 090 del 18 de enero de 2018, se fijan nuevos plazos para que los sujetos que resulten obligados realicen la inscripción de sus bases de datos, como lo indica la Superintendencia de Industria y Comercio (2018):

Los sujetos que continúan con el deber de registrar sus bases de datos son las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100 mil Unidades de Valor Tributario (UVT) y las entidades de naturaleza pública. Los plazos establecidos para realizar el registro de las bases de datos son tres: el primero de ellos es para las sociedades y entidades sin ánimo de lucro que tengan activos por más de 610.000 UVT, que deberán registrar sus bases de datos a más tardar el 30 de septiembre de 2018. El segundo plazo es para las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 y hasta 610.000 UVT, quienes tendrán plazo de realizar el registro hasta el 30 de noviembre de 2018. Por último, el tercer plazo corresponde a las entidades públicas, quienes tendrán plazo para registrar sus bases de datos hasta el 31 de enero de 2019 (Superintendencia de Industria y Comercio, 2018, p.1).

Así mismo, esta normativa redujo el número de sujetos, lo que evidencia una serie de deficiencias en la divulgación de la información sobre el registro de las bases y la claridad que tienen los sujetos obligados de la misma, de igual manera es evidente que aún se sigue almacenando y tratando información personal sin la autorización de sus titulares, lo que se evidencia en prácticas cotidianas como el ofrecimiento de productos y servicios.

Precisamente debido a lo anterior, el capítulo final de este artículo de reflexión se centra en determinar los retos que tiene Colombia en el marco de la protección al derecho de habeas data de todos los individuos en el país.

3. Retos para Colombia frente a la protección de datos personales.

Es importante destacar que Colombia ha expedido una normativa amplia respecto de la protección de datos personales, así mismo es notorio que existe un verdadero compromiso por parte de la Superintendencia de Industria y Comercio frente a la facultad sancionatoria que se le concedió frente a los establecimientos públicos y privados que incumplan con la Ley de protección de datos personales y las normas que lo complementan.

Ahora bien, si bien es cierto que a la fecha Colombia ha mejorado en el ámbito de protección de datos personales, es necesario que ciertos aspectos sean exigidos con mayor vehemencia,

con el fin de que la Ley de protección de datos, cumpla con sus fines. Como indica Alvarino (2017) un aspecto que es un reto dentro del derecho a la protección de datos es obligatoriedad de mediación de una autorización por parte del titular de los datos, que se considera el visto bueno de este para manejo, custodia y divulgación de sus datos personales.

Respecto de la autorización para el tratamiento de datos personales, la Ley fue clara en determinar que esta hace referencia al consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales (Superintendencia de Industria y Comercio, 2014, p.7).

Por lo tanto, es claro que la autorización de tratamiento de datos personales puede constar por escrito, o darse de manera verbal, o mediante conductas inequívocas del titular de la información, las cuales permiten concluir a los responsables que se otorgó la autorización, no obstante, el responsable del tratamiento de datos debe estar en capacidad de demostrar la autorización del titular de los datos personales en el caso que se presente una queja en contra de este.

En este sentido, es necesario castigar el aprovechamiento de entidades privadas de información considerada como datos públicos, para aspectos comerciales, ya que debe considerarse como un acto que va en contra de los principios mencionados en la Ley 1581 de 2012.

Es necesario, que se dé por terminada la fase de implementación de la norma y se finalice el plazo de registro de las bases de datos personales, teniendo en cuenta que han pasado 6 años de la expedición de la Ley 1581 de 2012, en esa medida a la fecha ya tendría que haber claridad sobre las bases de datos que requieren registro y las que no.

Por lo tanto, debe abrirse paso la verdadera protección del derecho al habeas data y la aplicación de multas y sanciones a las empresas y organizaciones que no realicen un tratamiento adecuado de la información que han recolectado, lo anterior para garantizar de manera real el derecho fundamental de cada ciudadano a la intimidad.

En segundo lugar, es notorio que, en el campo de los sujetos obligados en Colombia, hace falta ampliar la obligatoriedad de registro de bases de datos y política de tratamiento de datos

personales a empresas privadas, ya que la vigilancia y control de estas, es menor, teniendo en cuenta que tiene la potestad de regular la manera en que tratan los datos, en cumplimiento de los principios dados en la Ley.

Respecto de lo anterior, García (2015) ha señalado lo siguiente:

(...) aunque Colombia estableció la existencia de normas vinculantes que les permitan tanto a los gremios como a las empresas privadas la construcción de sus propias normas que regulen el tratamiento de los datos personales, siempre y cuando se enmarquen dentro de los principios y los lineamientos de la Ley de Protección de Datos Personales, no conminó, como sí lo hizo España, a que dichas normas tipo, o normas autovinculantes, fueran registradas en el RNBD, y dos años después de promulgada la Ley 1581 de 2012, el tema sigue sin regulación (p.154).

En ese sentido, hay que fijar obligaciones concretas respecto de todas las entidades públicas y todas las empresas privadas que tengan bajo su custodia el tratamiento de estos datos, ya que la integralidad del derecho al habeas data y a la intimidad de cada individuo debe ser una obligación tanto de las entidades públicas como de aquellas privadas, y en ese orden de ideas el seguimiento y la vigilancia debe darse con los mismos criterios.

Conclusiones

Es importante comenzar por reconocer que en el ámbito colombiano se ha logrado evidenciar un verdadero compromiso por parte de la Superintendencia de Industria y Comercio frente a la protección de datos personales y la facultad sancionatoria que se le concedió frente a los establecimientos públicos y privados que incumplan con la Ley de protección de datos personales y las normas que lo complementan.

No obstante, si bien en Colombia la legislación expedida ha hecho que exista una mejoría en el ámbito de protección de datos personales, es necesario que se implemente la Ley en su totalidad y se dejen de conceder plazos extensivos a una obligación conocida por las entidades públicas y privadas desde la expedición de la Ley, es decir el año 2012.

En este sentido, la primera debilidad que se observa en materia de protección de datos personales en Colombia es precisamente la incertidumbre que se ha generado en el marco de la implementación de la ley, por la extensión de plazos de registro de las bases de datos y la poca claridad que existe respecto de las bases que deben ser objeto de dicho registro.

De igual manera, si bien en la mayoría de los casos, se presenta la autorización del titular para el tratamiento de la información de acuerdo con lo dispuesto en la política de tratamiento de datos del establecimiento público o privado, la divulgación de la información con otros establecimientos sigue siendo un problema que no parece tener solución.

En la actualidad es relevante el número de quejas que se presentan día a día por la divulgación de datos personales, en este sentido si bien las multas si reflejan una inspección, vigilancia y control efectivo por parte de la Superintendencia de Industria y Comercio, las órdenes para corrección, eliminación y supresión de datos personales no es concordante si lo que se busca es garantizar el derecho a los individuos a la protección de datos personales.

Es necesario castigar el aprovechamiento de entidades privadas de información considerada como datos públicos, para aspectos comerciales, ya que debe considerarse como un acto que va en contra de los principios mencionados en la Ley 1581 de 2012. Es necesario, que se dé por terminada la fase de implementación de la norma y se finalice el plazo de registro de las bases de datos personales, teniendo en cuenta que han pasado 6 años de la expedición de la Ley 1581 de 2012, en esa medida a la fecha ya tendría que haber claridad sobre las bases de datos que requieren registro y las que no.

De igual manera, es plausible que se estudien los estándares en protección de datos que puedan mejorarse a partir de la regulación internacional y que tengan el fin de proteger el derecho a la intimidad de los ciudadanos, generando a partir de las tecnologías de la información una protección a aquellos datos que se consideran sensibles y que estén alojados en servidores que garanticen su confidencialidad.

Por lo tanto, debe abrirse paso a la verdadera protección del derecho al habeas data y la aplicación de multas y sanciones a las empresas y organizaciones que no realicen un

tratamiento adecuado de la información que han recolectado, lo anterior para garantizar de manera real el derecho fundamental de cada individuo a la intimidad.

Referencias

- Agudelo, Ó. A. (2018). Los calificativos del derecho en las formas de investigación jurídica. En Ó. A. Agudelo-Giraldo, J. E. León Molina, M. A. Prieto Salas, A. Alarcón-Peña & J. C. Jiménez-Triana. La pregunta por el método: derecho y metodología de la investigación (pp. 17-44). Bogotá: Universidad Católica de Colombia.
- Alvarino, I. M. (2017). Defensa del usuario de servicios de comunicaciones en Colombia: un camino tortuoso en la era digital. *Revista Jurídica Mario Alario D'Filippo*, 9(17), 169-184.
- Bautista Avellaneda, M. E. (2015). El derecho a la intimidad y su disponibilidad pública. Bogotá: Universidad Católica de Colombia
- Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. *Estudios Constitucionales*, 3(2), 85-139. Recuperado de <https://www.redalyc.org/pdf/820/82030204.pdf>
- Becerra, J., Sánchez Acevedo, M. E., Torres Ávila, J., García Vargas, C. B. & Cotino Hueso, L. (2015). El derecho a la protección de datos personales y la responsabilidad de la administración pública en el tratamiento de datos personales. En J. Becerra, M. E. Sánchez Acevedo, J. Torres Ávila, C. B. García Vargas & L. Cotino Hueso. (2015). La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC). Bogotá: Editorial Universidad Católica de Colombia.
- Buitrago Botero, D. M. (2016). El valor de los datos personales en Colombia. *Revista CES Derecho*, 7(1), 1-2. Recuperado de http://www.scielo.org.co/scielo.php?pid=S2145-77192016000100001&script=sci_arttext&tlng=en
- Castro, Á. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus: Revista Especializada en Sociología Jurídica y Política*, 10(1), 113-133. Recuperado

https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/view/1178/1928

Fernández Villazón, L. A. (2016). El nuevo reglamento europeo de protección de datos. Foro. Revista de Ciencias Jurídicas y Sociales. Nueva época. Edición Online: <http://digibuo.uniovi.es/dspace/bitstream/10651/45268/1/53399-101180-2-PB.pdf>.

Galvis, L. (2012). Protección de datos en Colombia, avances y retos. Revista Lebre, 4(4), 195-214. Recuperado de <http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336>

Galvis Cano, L., & Salazar Bautista, R. L. (2019). Alcance del derecho al olvido en el tratamiento de datos personales en Colombia. Verba Iuris, (41).

García Vargas, C. (2015). La incidencia del modelo español en el registro nacional de bases de datos colombiano como herramienta de supervisión y control. En: J. Becerra, G. D. Flórez Acero, C. García Vargas, C. Rojas Orjuela Vargas, M. E. Sánchez Acevedo & J. Torres Ávila. El derecho y las tecnologías de la información y la comunicación (TIC) (pp. 101-160). Bogotá: Universidad Católica de Colombia

Gil, J. C. (2017). El debido proceso en la Ley de Habeas Data. CES Derecho, 8(1), 191-204. Recuperado de <http://revistas.ces.edu.co/index.php/derecho/article/view/4269>

Hernández, R. (2008). Delimitación de los derechos a la intimidad y de información en la doctrina y jurisprudencia costarricense. Estudios Constitucionales, 6 (1), 85- 102. Recuperado de <https://www.redalyc.org/html/820/82060105/>

Iraburu, M. (2006). Confidencialidad e intimidad. In Anuales del Sistema Sanitario de Navarra (Vol. 29, pp. 49-59). Recuperado de <http://scielo.isciii.es/pdf/asisna/v29s3/original5.pdf>

Maqueo, M., Moreno, J., & Recio, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia), 30(1), 77-96. Recuperado de <https://dx.doi.org/10.4067/S0718-09502017000100004>

- Organización de Estados Americanos. (2019). Protección de Datos Personales. Informe OEA. Departamento de Derecho Internacional (DDI). Recuperado de http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp
- Puldaín, V. (2017). El futuro marco legal para la protección del acceso a los datos. Revista Ibero-Latinoamericana de Seguros, 26(47). Recuperado de <https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/21178>
- Remolina, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? International Law: Revista Colombiana de Derecho Internacional, (16). Recuperado de <http://www.redalyc.org/html/824/82420041015/>
- Rojas Bejarano M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Novum Jus, 8(1), 107-139. <https://doi.org/10.14718/NovumJus.2014.8.1.6>
- Romero, X. L. (2008). Alcance del Derecho a la Intimidad en la Sociedad Actual, El. Rev. Derecho del Estado, 21, 209. Recuperado de <https://heinonline.org/HOL/LandingPage?handle=hein.journals/revderest21&div=13&id=&page=>
- Superintendencia de Industria y Comercio. (2014). Protección de Datos Personales. Bogotá: Imprenta Nacional. Recuperado de <http://www.sic.gov.co/sus-derechos>
- Superintendencia de Industria y Comercio. (2018). Registro Nacional de Bases de Datos. Bogotá: Imprenta Nacional. Recuperado de <https://www.sic.gov.co/registro-nacional-de-bases-de-datos>
- Torres Ávila, J. (2016). Estrategias de implementación de las obligaciones del derecho de acceso a la información pública y la transparencia en el ámbito local. En J. Torres Ávila. La transparencia y el buen gobierno: una perspectiva desde los derechos humanos y las obligaciones de los gobiernos locales (pp. 89-104). Bogotá: Universidad Católica de Colombia.